Commonwealth Information Security Council
Risk Management Committee Meeting
August 16, 2010
2:00 pm CESC

Risk Management Committee members attending:

Ed Miller, DOA, Co-Chair
Goran Gustavsson, APA, Co-Chair
Jack Spooner, DOA
Ross McDonald, DSS *
Bob Auton, DJJ *
Joshua Cole, Dept of Aviation *

* (Teleconference to CESC)

Risk Management Committee members absent:

Jeremy Greenwood, TRS

Also Attending:

John Green, COV CISO
Mauri Shaw, VITA CRSM

Topic: Risk Management – Discussions

Discussion from the prior Security Council meeting (August 16) – assessing whether the RA guideline and Security Audit Standard need changing and are doable. Audit findings indicate the following:

- Some sensitive systems may not be really representative of the agencies most important processes and procedures.

- Agency risk identification and review processes vary (e.g. some agencies may not declare any of their applications as sensitive for Risk Assessing and some agencies may declare all of their applications sensitive and some agencies are between these two extremes.

- Some application controls may address or provide the same infrastructure and controls that are under review for other sensitive systems – reviewing and reporting on these controls will impact the reporting on similar systems. (e.g. Data Base Controls).

- Additional manual controls can help mitigate the vulnerabilities that are found. These considerations could potentially impact future risk assessment reviews, (e.g. "… not all agency declared sensitive systems need to be reviewed/risk assessed if they are found to have identical operations and controls).

- Corrective Action Plans – an agency may report audits of sensitive systems and their Corrective Action Plans based upon findings from prior APA audits. The linking of prior APA reviews/audits may or may not realistically indicate that the agency has complied with the requirements of the Security Audit Standard. General comment.

- Auditing each sensitive system every 3 years does not appear doable with the cutbacks on audit staff and budget to hire out the review. Additional review of the audit requirement and the risk Assessment requirements should be scheduled to further align them with the current COV environment.

Discussion of the need for a COV Questionnaire - reporting COV wide sensitive system findings/issues/vulnerabilities/risks and potential related control recommendations so the CISO could present an Enterprise-wide solution(s) – moving these recommendations forward through management and if approved, requesting funding for solution resources.